IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Mark L. Wilkinson, Ronald J. Miller, Michael J. McDaniels		
Assignee:	Mirage Networks, Inc.		
Title:	Deterring Network Incursion		
Serial No.:	10/676,637	Filing Date:	October 1, 2003
Examiner:	Unassigned	Group Art Unit:	2143
Docket No.:	MIR0003US		

Austin, Texas
January 23, 2006

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION TO MAKE SPECIAL UNDER 37 CFR §1.102(d)

Dear Sir:

The applicants hereby petition pursuant to 37 CFR §1.102(d) and MPEP § 708.02(VIII) to make the above-identified application special. Please charge Deposit Account No. 502306 for the fee of $130.00 for this petition as set forth in 37 CFR §1.17(h).

Should the Office determine that all the claims presented are not obviously directed to a single invention, the applicants will make an election without traverse as a prerequisite to the grant of special status.

The applicants respectfully submit that a pre-examination search has been performed by a professional search firm in the following classes/subclasses:

Class	Subclasses
709	223, 224, 225
713	201
726	13, 22, 23

Enclosed is a preliminary amendment which requests to amend claims 1, 3, 5, 6, 11, 16, 42, 44, 47-49, 57, 59, 62-64, 72, 74, and 77-79. The references have been evaluated herein in light of the claims as amended therein.

Also enclosed are copies of the following references which are presently believed to be, from any previously filed Information Disclosure Statement, the most closely related to the subject matter encompassed by the claims:

Patent/Publication No.	Inventor	Date
5,884,025	Baehr et al.	March 16, 1999
2004/0044912 A1	Connary et al.	March 4, 2004 (Publication Date)
6,725,378	Schuba et al.	April 20, 2004

Detailed Discussion of the References

U.S. Patent No. 5,884,025 (Baehr et al.) discloses a system for screening data packets as they arrive on a network for security threats. (See Baehr, Abstract.) Baehr's system intercepts a packet, screens the packet based on various pieces of information, and determines an action to take regarding the packet including dropping, blocking, altering, or allowing the packet. (*Id.*; Baehr, column 2, lines 10-49)

As the title "System for Packet Filtering of Data Packets at a Computer Network Interface" suggests, Baehr's system is designed to control packets flowing into (and out of) a protected private network. (See Baehr, column 7, lines 5-16 and column 8, lines 27-37.) If a packet is received from an external source address that is regarded as a threat, the packet is prevented from entering the private network. (See *id.*; see also column 9, lines 60 - 67.) No further examination of the packet is performed before determining a response to the packet, as required by independent claims 1, 42, 57, and 72. Furthermore, Baehr's system is limited to dealing with external threats. Baehr's system does nothing to prevent distribution of infected packets internally after the network has been infected.

In contrast, the claimed invention examines packets before determining a response, even if the source address is considered to be a threat. Furthermore, as claimed in dependent claims 5, 6, 11 and 16, *inter alia*, the source address sending a packet can be considered to be a threat even though the source address is internal to the local network. If a local device has been determined to be a threat, the present invention prevents distribution of infected packets inside the network. For example, other local devices are prevented from communicating with the local threat by reinitializing the other local devices' ARP tables with a synthetic hardware address for the internal local threat (as claimed in claim 11). In addition, communication from the local threat to other devices is prevented by causing the local threat's ARP table to be reinitialized with synthetic addresses for other local devices (as claimed in claim 16).

Consequently Baehr does not teach these limitations of claims 1, 42, 57, and 72. Therefore, independent claims 1, 42, 57, and 72 and respective dependent claims 2-40, 43-55, 58-70, and 73-85 are allowable for at least this reason.

Furthermore, replacing a synthetic hardware address with a valid hardware address and sending the packet are required by independent claims 41, 56, 71, and 86. Baehr does not teach the concept of a synthetic hardware address or of replacing a synthetic hardware address with a valid hardware address. Consequently, independent claims 41, 56, 71, and 86 are allowable over Baehr for at least this reason.

U.S. Patent No. 6,725,378 (Schuba et al.) discloses a system and method for protecting networks from intrusions, specifically denial of service attacks. The system includes a means for monitoring incoming data on a network, determining if a packet is suspect, and categorizing the packet source address as unacceptable, suspect, or acceptable (See Schuba, column 2, lines 1-5, and Fig. 4). If a packet is found to have an unacceptable source address, the packet is placed in an "unacceptable address state." (*Id.*) As described therein, the unacceptable address state "do[es] not involve any appreciable amount of processing beyond the states shown in Fig. 4." (See Schuba, column 9, lines 16-20 and 33-37.) Fig. 4 step 72 indicates that a reset message is sent to close the spurious connection to the unacceptable source address. (See Schuba, column 9, lines 23-32.) No further processing of the packet is performed. (See Schuba, column 9, lines 16-20 and 33-37.)

In contrast, in the claimed invention, even if the source address is classified as a threat initially, the packet is nevertheless examined and a response to the packet is determined based upon the examination and whether the source address is a threat. Examining the packet and determining a response to the packet based upon the examination and whether the source address is a threat are required by independent claims 1, 42, 57, and 72. Consequently, independent claims 1, 42, 57, and 72 and respective dependent claims 2-40, 43-55, 58-70, and 73-85 are allowable over Schuba for at least this reason.

Similarly, examining the packet and performing a response that includes replacing a synthetic hardware address with a valid hardware address and sending the packet are required by independent claims 41, 56, 71, and 86. Schuba does not teach the concept of a synthetic hardware address or of replacing a synthetic hardware address with a valid hardware address. Consequently, independent claims 41, 56, 71, and 86 are allowable over Schuba for at least this reason.

U.S. Patent Application 2004/0044912 (Connary et al.) discloses a method for determining a network security threat. Network devices are monitored to aggregate all event data generated by monitored devices to provide a network ranking of all network activity. (See Connary, Abstract.) A threat level for a given host is determined by a threat weighting assigned to that host and a threat weighting assigned to that host's netblock. (*Id.*)

In one embodiment, a sensor detects network events and records data regarding such events. (See Connary, paragraph [0008].) The event data can include, for example, information about the sensor detecting the event, source and destination IP addresses associated with the event, source and destination ports, and/or the type of event (e.g., "Get request," accept, reject, etc.). (*Id.*) Event data also includes a time and date of receipt that a management module received the event data. (Connary, paragraph [0009].)

Applicants respectfully submit that the analysis performed by Connary's system requires examination of more than one packet. Connary's system accumulates event data and processes the event data by multiple modules before the nature of the threat posed by the event data can be determined. (See Connary, paragraphs [0008] through [0010].) Consequently, determining a response to a given packet, as claimed, requires more information than is available from examining that given packet and determining whether the source address is a threat. Accordingly, independent claims 1, 42, 57, and 72, and respective dependent claims 2-40, 43-55, 58-70, and 73-85 are allowable over Connary for at least this reason.

Replacing a synthetic hardware address with a valid hardware address and sending the packet are required by independent claims 41, 56, 71, and 86. As with the Baehr and Schuba references, Connary does not teach the concept of a synthetic hardware address or of replacing a synthetic hardware address with a valid hardware address. Consequently, independent claims 41, 56, 71, and 86 are allowable over Connary for at least this reason.

Conclusion

In summary, Applicants respectfully submit that none of the references located during the pre-examination search, or otherwise made of record by Applicants, teaches or suggests (at least) examining a packet and determining a response to the packet based upon the examination and whether the source address qualifies as a threat. Accordingly, Applicants respectfully submit that claims 1-86 are allowable over all of the above references.

Accordingly, Applicants respectfully request that this petition be granted, and that the present application receive expedited examination. Should any issues remain that might be subject to resolution through a telephonic interview, the Office is requested to telephone the undersigned.

Express Mail Label No:
EV 643139286 US

Respectfully submitted,

D'Ann Naylor Rifai
Attorney for Applicant(s)
Reg. No. 47,026
512-439-5086
512-439-5099 (fax)